Information and Management Sciences
Volume 3, Number 2, pp.93-100, 1991

Group-Oriented Secure Communications Based on the RSA Scheme

Tzonelih Hwang
National Cheng Kung University
R.O.C.

Abstract

A practical protocol based on the RSA scheme is proposed to solve several open problems in the group oriented cryptography. the protocol allows the information sender to send a confidential data to the destination group without knowing the group's organization and policy. The destination company, upon receiving the message, this protocol is particularly useful in large group oriented networks. Companies in the network can communicate in private with each other knowing only the public keys.

Keywords: Cryptography, Group, RSA Public-key System, Secure Communication.